Zentrum Digitale Souveränität

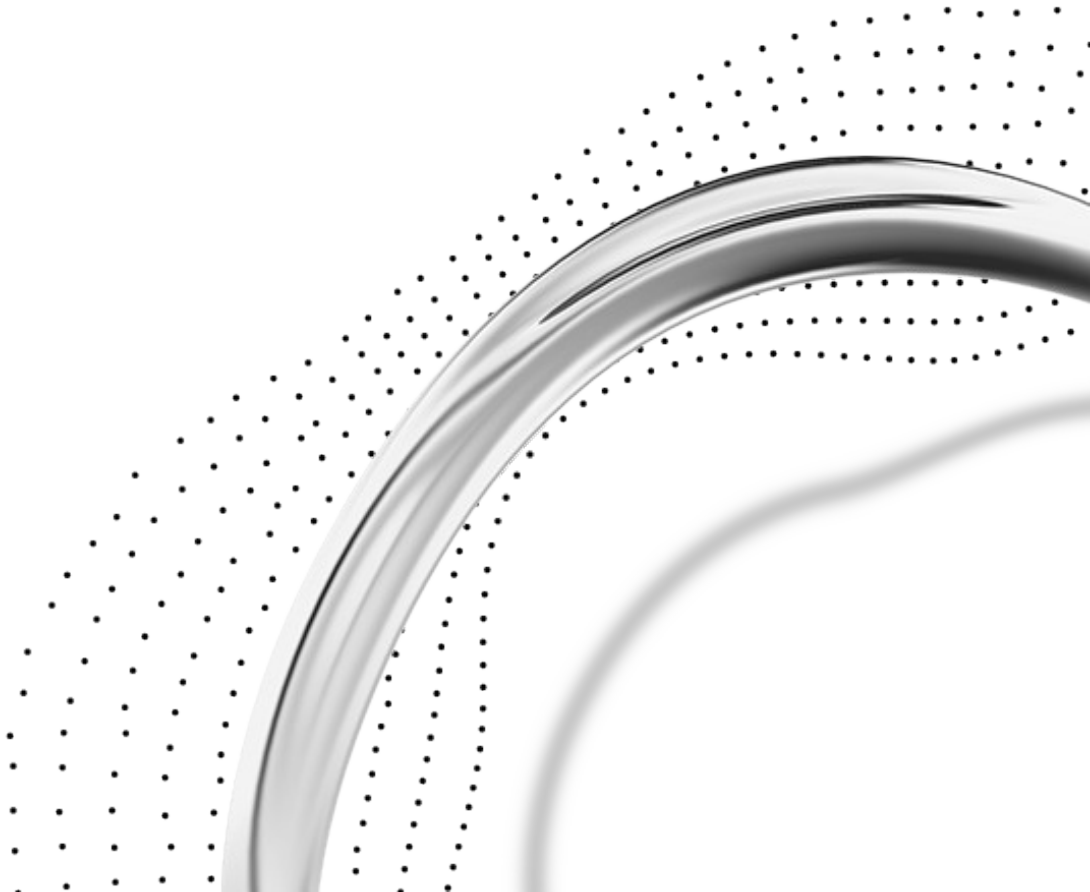
openDesk Software-as-a-Service

Datenschutzkonzept

Dokumentation im Sinne der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO

Stand: 5. September 2025

Version: 0.3



Inhaltsverzeichnis

1. Zielsetzung Datenschutzkonzept....4

1.1. Datenschutzkonzepte im Allgemeinen....4

1.2. Datenschutzkonzept als Auftragsverarbeiter....4

2. Beschreibung der Datenverarbeitung....5

2.1. Inhaltlicher Prozess....5

2.2. Eingesetzte Technik....6

2.2.1. Infrastruktur (Hardware)....6

2.2.2. Anwendung (Software)....6

2.3. Beteiligtes Personal....6

2.4. Verantwortliche....7

2.5. Auftragsverarbeiter....7

3. Rechtsgrundlagen....8

3.1. Rechtsgrundlage aus Perspektive der Auftragsverarbeiter....8

3.2. Rechtsgrundlage für die openDesk-Nutzung....8

3.3. Rechtsgrundlage für Verarbeitung besonders schützenswerter Daten (Art. 9 DSGVO)....9

4. Angaben für Verzeichnis der Verarbeitungstätigkeiten....10

4.1. Datenarten....10

4.2. Zweck der Verarbeitung....11

4.3. Kategorien betroffener Personen....11

4.4. Kategorien von Datenempfängern....11

4.5. Drittstaatentransfers....11

4.6. Löschfristen....11

4.7. Allgemeine Beschreibung der Schutzmaßnahmen....11

5. Angaben für Datenschutzinformation....12

5.1. Beschreibung....12

5.2. Datenkategorien....13
5.3. Datenempfänger (ggf. Drittstaatentransfer)....13
5.4. Zweck und Rechtsgrundlage....13
5.5. Speicherdauer....14

6. Begleitende Dokumentation....14

7. Datensicherheit und Risikoadäquanz (Art. 24, 25, 32 DSGVO)....14

7.1. Einleitung Risiko und Adäquanz....14
7.1.1. Fokus auf Betroffene....15
7.1.2. Datenschutzrisiken und Schutzbedarf nach Informationssicherheit....15
7.1.3. Ergänzende Gewährleistungsziele....16
7.1.4. Definition Risiko....16
7.2. Datenschutzrisiken durch diese Verarbeitung....16
7.3. Schutzmaßnahmen und Zuordnung zu den Risiken....17
7.4. Feststellung Risikoadäquanz....18

8. Datenschutzfolgenabschätzung (Art. 35 DSGVO)....18

9. Fazit....19

1. Zielsetzung Datenschutzkonzept

1.1. Datenschutzkonzepte im Allgemeinen

Das Datenschutzkonzept („DSK“) dient als Rechenschaftsnachweis gemäß Art. 5 Abs. 2 DSGVO. Datenschutzrechtlich Verantwortliche sind durch die Datenschutz-Grundverordnung („DSGVO“) auf die Einhaltung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DSGVO verpflichtet. Diese Grundsätze finden ihre Ausprägung in den einzelnen Vorgaben der DSGVO und dem Datenschutzrecht der Mitgliedsstaaten (z.B. BDSG) sowie den Betroffenenrechten.

Das DSK ist kein abschließendes Dokument zur Rechtmäßigkeit der Datenverarbeitung; es verweist auf ergänzende Dokumente. Die ergänzenden Dokumente umfassen eigenständige Themenbereiche (wie z.B. ein Datensicherungskonzept) oder erfüllen selbstständige Dokumentationsanforderungen (wie z.B. der Eintrag für das Verzeichnis der Verarbeitungstätigkeiten). Einige der ergänzenden Dokumente werden innerhalb des DSK als Anlage zu diesem geführt; auf andere Dokumente wird aus dem DSK heraus verwiesen.

Im Sinne einer effizienten Lesbarkeit werden Normen und rechtliche Konzepte hinter diesen Normen, wie sie z.B. durch die Rechtsprechung oder Arbeit der Datenschutzaufsichtsbehörden entwickelt worden sind, nur im notwendigen Umfang innerhalb des DSK vorgestellt. Das DSK richtet sich an eine Zielgruppe, bei der eine grundsätzliche Datenschutzexpertise vorausgesetzt wird.

Das DSK ist nicht als Einführung ins Datenschutzrecht angelegt, sondern als Nachweis, dass die datenschutzrechtlichen Anforderungen bei dem hier vorgestellten Datenverarbeitungsprozess eingehalten wurden.

1.2. Datenschutzkonzept als Auftragsverarbeiter

Die Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO trifft den Verantwortlichen für die Datenverarbeitung nach Art. 4 Nr. 7 DSGVO. Diese DSGVO-Verantwortlichkeit liegt für einen browserbasierten Clouddienst – nachfolgend Software-as-a-Service („SaaS“) genannt – wie openDesk bei den Organisationen, die openDesk-Zugänge nutzen. Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung GmbH („ZenDiS“) ist Betreiber des openDesk-SaaS-Dienstes und stellt diesen als Auftragsverarbeiter nach Art. 28 DSGVO zur Verfügung.

Dieses DSK wird dementsprechend nicht aus der Perspektive eines Verantwortlichen, sondern eines Dienstleisters zur Verfügung gestellt. Häufig werden solche Dienstleister-

oder Betreiber-DSK Rahmendatenschutzkonzept genannt. Dieses Dokument verwendet den Begriff DSK.

2. Beschreibung der Datenverarbeitung

2.1. Inhaltlicher Prozess

Dieses DSK betrifft die Bereitstellung eines Mandanten der Anwendung openDesk (siehe eine Demo-Version auf https://demo.opendesk.eu). openDesk ist eine browserbasierte Onlineanwendung (Software-as-a-Service/ SaaS). openDesk ist ein für den öffentlichen Sektor entwickelter digitaler Arbeitsplatz bestehend aus webbasierten Open-Source-Modulen mit vielen Funktionen, die Mitarbeiterinnen und Mitarbeitern aus dem öffentlichen Sektor benötigen.

openDesk umfasst Anwendungen aus folgenden Gruppen (in Klammern die konkreten Open-Source-Module):

- Kommunikation & Organisation: E-Mail, Kalender, Kontakte & Aufgaben (OX AppSuite)
- Produktivität: Dateien (Nextcloud)
- Produktivität: Diagramme (CryptPad mit diagrams.net)
- Produktivität: Weboffice (Collabora Online)
- Management: Projekte (OpenProject)
- Management: Wissen (XWiki)
- Direkte Kommunikation: Chat & Zusammenarbeit (Element mit Nordeck widgets)
- Direkte Kommunikation: Sofort-Videokonferenz (Jitsi)
- Portal (Univention)

Für jeden openDesk-Kunden wird ein eigenständiger openDesk-Mandant eingerichtet. Zu diesem Mandanten erhält der Kunde einen Mandanten-Administrationszugang, über den die zuständigen Personen beim Kunden weitere Nutzendenkonten einrichten können. Diese Konten ermöglichen den Nutzenden über einen Internetbrowser auf einem Gerät mit Internetzugang den Zugang zur SaaS-Anwendung.

2.2. Eingesetzte Technik

2.2.1. Infrastruktur (Hardware)

Der openDesk-Mandant wird aus den Rechenzentren des Auftragsverarbeiters STACKIT gehostet.

2.2.2. Anwendung (Software)

Der openDesk Mandant ist eine Anwendungsinstanz, die als openDesk-Instanz auf einem Portal von Univention aufbaut. An die Portalverwaltung knüpfen die einzelnen Funktionsanwendungen an, die in der Beschreibung des inhaltlichen Prozesses bereits genannt worden sind.

2.3. Beteiligtes Personal

Das ZenDiS lässt die Anwendung von dem Generalunternehmer B1 betreiben, der sowohl die technische Bereitstellung (Hosting) durch den Rechenzentrumsanbieter STACKIT steuert wie die fortlaufende Anwendungsentwicklung im Austausch mit der Open-Source-Community im Allgemeinen und den Gruppen bzw. Unternehmen hinter den Anwendungsbausteinen im Konkreten.

Die Entwickelnden als Partner für die einzelnen Anwendungsbausteine haben keinen Zugang zu personenbezogenen Daten in den produktiven openDesk-Mandanten. Die Mitarbeitenden von B1 stehen als Support-Dienstleister zur Verfügung. Ausgewählte Administratoren bei B1 haben technisch Zugang zu den Daten innerhalb der Mandanten. Technisch haben auch die entsprechend berechtigten Administratoren von STACKIT Zugang zu den Daten. Jedoch ist sowohl den Administratoren bei B1 wie noch viel mehr bei STACKIT der Zugriff auf Daten innerhalb eines Mandanten nur im Falle einer entsprechenden Supportanfrage gestattet.

Die Mitarbeitenden des ZenDiS haben keinen Zugang zu den Daten innerhalb der openDesk-Mandanten. Da anwendungsbezogene Supportaufgaben vollständig über den Generalunternehmer laufen, bedarf es für ZenDiS-Mitarbeitende keiner Zugangsmöglichkeiten.

Alle Mitarbeitenden sind durch ihre Arbeitgeber auf die ihren Aufgaben und Zugangsrechten entsprechende Vertraulichkeit verpflichtet worden. Die Dienstleister des ZenDiS sind durch entsprechende Verträge auf die Vertraulichkeit und damit einhergehende Schutzmaßnahmen verpflichtet.

Verantwortliche Stellen und Verantwortungsbereiche

Die DSGVO kennt neben der alleinigen (oder getrennten) Verantwortlichkeit die gemeinsam Verantwortlichen nach Art. 26 DSGVO und die weisungsgebundenen Dienstleister als Auftragsverarbeiter nach Art. 28 DSGVO.

2.4. Verantwortliche

Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO sind diejenigen, die über Zwecke und Mittel der Verarbeitung personenbezogener Daten bestimmen.

Verantwortliche für den Betrieb eines openDesk-Mandanten ist die Organisation, die den Mandanten beim ZenDiS in Auftrag gegeben hat. Die verantwortlichen Personen beim ZenDiS-Auftraggeber bestimmen, zu welchen Zwecken welche Daten über den openDesk-Mandanten verarbeitet werden sollen und wer Zugang zu diesen Daten erhält (z.B. durch das Bereitstellen eines entsprechenden openDesk-Zugangskontos).

2.5. Auftragsverarbeiter

Auftragsverarbeiter nach Art. 4 Nr. 8 und Art. 28 DSGVO ist, wer personenbezogene Daten weisungsgebunden verarbeitet. Auftragsverarbeiter haben einen eigenen Entscheidungsspielraum mit Blick auf Details der technischen Infrastruktur, des eingesetzten Personals, der genutzten Unterauftragnehmer und der angewendeten Sicherheitsmaßnahmen. Grundsätzliche Veränderungen an der Infrastruktur, den vereinbarten Schutzmaßnahmen nach Art. 32 DSGVO und den eingesetzten Unterauftragnehmern sind aber nur mit Zustimmung oder auf Wunsch des Verantwortlichen zulässig.

Zentraler Auftragsverarbeiter für die Bereitstellung des openDesk-Dienstes ist aus Sicht der Verantwortlichen das ZenDiS.

Als Unterauftragnehmer des ZenDiS kommt für openDesk folgender Auftragsverarbeiter zum Einsatz:

1. B1 Systems GmbH als Generalunternehmer (Osterfeldstr. 7, 85088 Vohburg, https://www.b1-systems.de)

Als Unterunterauftragnehmer hinter B1 Systems GmbH kommt für openDesk folgender Auftragsverarbeiter zum Einsatz:

1. STACKIT GmbH & Co. KG als Hosting-Dienstleister (Rechenzentrumsbetreiber; Stiftsbergstr. 1, 74172 Neckarsulm, https://www.stackit.de)

Mit den Auftragsverarbeitern sind Auftragsverarbeitungsverträge („AV-Verträge“) nach Art. 28 DSGVO abzuschließen. ZenDiS hat entsprechende Verträge geschlossen.

3. Rechtsgrundlagen

Jede Verarbeitung personenbezogener Daten durch einen Verantworltichen bedarf einer Rechtsgrundlage.

3.1. Rechtsgrundlage aus Perspektive der Auftragsverarbeiter

ZenDiS und die Unterauftragnehmer des ZenDiS müssen für die Verarbeitung personenbezogener Daten innerhalb des openDesk-Mandanten keine Rechtsgrundlage nachweisen. Diese Pflicht trifft allein die DSGVO-Verantwortlichen, also die Inhaber/ Betreiber der openDesk-Mandanten.

3.2. Rechtsgrundlage für die openDesk-Nutzung

Verantwortliche müssen sich für die Verarbeitung personenbezogener Daten auf mindestens eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO berufen können. Die Rechtsgrundlagen orientieren sich an der Zwecksetzung der Datenverarbeitung.

Die Zwecksetzung innerhalb einer identischen Verarbeitungstätigkeit kann mit Blick auf unterschiedliche Kategorien von Betroffenen unterschiedlich ausfallen.

Beispiel: Schickt Behördenmitarbeiterin A eine E-Mail an Sachverständige B und erwähnt in der E-Mail C als Antragstellerin und D als Angehörige der Antragstellerin, dann greift als Rechtsgrundlage:

- für A ihr Dienstvertrag und damit zumindest Art. 6 Abs. 1 lit. b (Vertragserfüllung) und evtl. auch Art. 6 Abs. 1 lit. c (Rechtliche Verpflichtung aus dem öffentlich-rechtlichen Dienstverhältnis)
- für B ihre Beauftragung als Sachverständige und damit zumindest Art. 6 Abs. 1 lit. b (Vertragserfüllung) und abhängig von der gesetzlichen Ausgestaltung der Sachverständigeneinbindung auch Art. 6 Abs. 1 lit. c (Rechtliche Verpflichtung)
- für C im Rahmen ihrer Antragstellung Art. 6 Abs. 1 lit. c, da die Behörde gesetzlich verpflichtet ist, den Antrag zu bearbeiten

- für D in der sekundären Rolle als Angehörige Art. 6 Abs. 1 lit. e, soweit die Einbeziehung der Angehörigen im (öffentlichen) Interesse des ordnungsgemäßen Antrags- bzw. Verwaltungsverfahrens liegt.

Zusammenfassend lässt sich für die öffentliche Hand sagen, dass jede Verarbeitung personenbezogener Daten, die den Vorgaben und Standards des jeweiligen Verwaltungshandelns oder Dienstrechts entspricht, auch einer der Rechtsgrundlagen nach Art. 6 Abs. 1 lit. b, c oder e DSGVO entspricht. Das Datenschutzrecht stellt insoweit keine Anforderungen auf, die über Verwaltungs- oder Dienstrecht hinausgehen. Entscheidend ist aber, im Rahmen der Verhältnismäßigkeitsprüfung des jeweiligen Handelns auch das Grundrecht auf Datenschutz in die Angemessenheitsprüfung einzubeziehen und vor allem die Erforderlichkeit der Verarbeitung personenbezogener Daten zur Erreichung des legitimen Zwecks zu prüfen.

Diese Grundlogik gilt für alle Formen der Datenverarbeitung, die openDesk als digitaler Arbeitsplatz ermöglicht; also neben der Kommunikation per E-Mail auch die Erstellung und Speicherung von Dokumenten mit den Office-Anwendungen in openDesk, Videokonferenzen über openDesk oder die Verwaltung von Terminen, Kontakten, Aufgaben oder Projektzuständen.

Die Erfassung technischer Daten wie der IP-Adresse der Endgeräte der openDesk-Nutzenden ist technisch zwingend erforderlich, um die Onlineanwendung dem Endgerät der Nutzenden bzw. den darauf installierten Browsern zur Verfügung stellen zu können. Hinzu treten Pflichten des Verantwortlichen aus der Informationssicherheit zur Protokollierung.

3.3. Rechtsgrundlage für Verarbeitung besonders schützenswerter Daten (Art. 9 DSGVO)

Werden über openDesk auch besonders schützenswerte Daten nach Art. 9 Abs. 1 DSGVO verarbeitet, bedarf es zusätzlich zur Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO auch einer Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO. Auch die Rechtsgrundlagen nach Art. 9 Abs. 2 stehen im Einklang mit rechtmäßigem Verwaltungshandeln, so dass bei grundrechtskonformen Veraltungshandeln auch datenschutzkonformes Handeln gegeben ist. In Zweifelsfällen sollte das Verwaltungshandeln hinterfragt und dessen Grundrechts- und Datenschutzkonformität unter Einbeziehung von Zwecksetzung, Erforderlichkeit und Angemessenheit überprüft werden.

Es liegt im Verantwortungsbereich des openDesk-Mandantenbetreibers seine Beschäftigten und openDesk-Nutzenden auf eine grundrechts- und datenschutzkonforme Arbeit zu verpflichten und im erforderlichen Umfang zu schulen und mit entsprechenden Richtlinien und Handreichungen zu anzuleiten.

4. Angaben für Verzeichnis der Verarbeitungstätigkeiten

Die folgenden Angaben dienen für einen Eintrag in das Verzeichnis der Verarbeitungstätigkeiten („VVT“) des Verantwortlichen, also des Betreibers eines openDesk-Mandanten.

Verantwortliche genießen ein gewisses Maß an Ermessensfreiraum, welche einzelnen Verarbeitungsschritte eine ganzheitliche Verarbeitungstätigkeit bilden. Denkbar ist regelmäßig auch, das jeweilige Verwaltungsverfahren als Verarbeitungstätigkeit zu verstehen und den Einsatz der openDesk-Technologie als eines digitalen Arbeitsplatzes nur als einen Verarbeitungsschritt innerhalb einer größeren, ganzheitlich betrachteten Verarbeitungstätigkeit zu betrachten.

Wird die Nutzung von openDesk nur als ein Schritt verstanden, bedarf es keines eigenständigen Eintrags für den digitalen Arbeitsplatz in das VVT des Verantwortlichen. Dann genügt eine Nennung der Anwendung als Arbeitsmittel im Rahmen einer z.B. an konkreten Verwaltungstätigkeiten ausgerichteten Dokumentation.

4.1. Datenarten

Datenarten innerhalb der Nutzungsprotokollierung:

- IP-Adresse, von der aus openDesk aufgerufen wurde
- Datum und Uhrzeit des Zugriffs
- Objekte in openDesk, die im Browser aufgerufen werden
- Art und Version des Internetbrowsers
- Art und Version des Betriebssystems

Datenarten innerhalb der Anwendungsnutzung:

- Namen und Kontaktdaten (Adressen, Telefonnummern, E-Mail-Adressen)
- Kommunikations- und Rechercheinhalte (in E-Mails, Schreiben/ Akten, Notizen, Nachrichten, Videokonferenzen)
- Termine
- Bild-, Video- und Tonaufnahmen (als Dateien, die in openDesk gespeichert werden)

Abhängig vom Aufgabenbereich der openDesk-Nutzenden können die Kommunikations- und Rechercheinhalte personenbezogene Daten jeder Art umfassen, also auch besonders schützenswerte Daten nach Art. 9 DSGVO wie z.B. Gesundheitsdaten oder nach Art. 10 DSGVO zu Strafverfahren.

4.2. Zweck der Verarbeitung

Nutzung der openDesk-Anwendung als eines digitalen Arbeitsplatzes und aller darin enthaltenen Funktionen zu Kommunikation und Speicherung

Für die Nutzungsprotokollierung: Informationssicherheit in Form von Nachweisbarkeit ordnungsgemäßen Verwaltungshandelns sowie forensische Nachforschungen im Falle eines Verdachts auf Missbrauch der Anwendung oder eines Angriffs auf die Anwendung; statistische Analyse des Nutzungsverhaltens als Grundlage für Optimierungen der Anwendung

4.3. Kategorien betroffener Personen

- openDesk-Nutzende
- Personen ohne Zugang zu diesem openDesk-Mandanten, mit denen per E-Mail, Videokonferenz oder Nachricht kommuniziert wird (Kommunikationspartner)
- Personen, die in den in openDesk gespeicherten Daten unmittelbare oder mittelbare Erwähnung finden (Antragstellende, Angehörige, Sachverständige, Zeugen, beteiligte Personen jeder Art)

4.4. Kategorien von Datenempfängern

Auftragsverarbeiter (Anbieter ZenDiS und als Unterauftragnehmer Generalunternehmer B1 Systems und Rechenzentrum STACKIT)

4.5. Drittstaatentransfers

Kein Drittstaatentransfer.

4.6. Löschfristen

Die Löschfristen für die in openDesk gespeicherten Inhalte und die Protokollierungsdaten sind vom Betreiber des openDesk-Mandanten festzulegen und zu administrieren.

4.7. Allgemeine Beschreibung der Schutzmaßnahmen

Siehe TOMs im Auftragsverarbeitungsvertrag für openDesk, insbesondere die TOMs der Unterauftragnehmer, bei denen über Support-Leistungen (B1 Systems) und Hosting (STACKIT) die tatsächliche Verarbeitung personenbezogener Daten erfolgt

5. Angaben für Datenschutzinformation

Die nachfolgenden Angaben dienen der Informationspflicht des Verantwortlichen den Personen gegenüber, denen der Verantwortliche einen Zugang zu seinem openDesk-Mandanten zur Verfügung stellt.

Die Information der Personen ohne Zugangskonto zum openDesk-Mandanten ist anhand der jeweiligen Beziehung diesen Personen gegenüber zu erstellen und auf passende Weise zur Verfügung zu stellen. Diese Informationsleistung bemisst sich in erster Linie nach den Gegebenheiten der jeweiligen Verwaltungstätigkeit, in deren Rahmen die Daten der Personen erfasst und verarbeitet werden. Insbesondere das Thema Aufbewahrungszeit knüpft an die Vorgaben des jeweiligen fachlichen Prozesses an.

5.1. Beschreibung

Datenverarbeitung durch die Nutzung einer browserbasierten Onlineanwendung: Damit ein Webserver openDesk Ihrem Browser zur Verfügung stellen kann, muss der Server technische Daten über Ihr dafür genutztes Gerät, Ihren Browser und Ihren Internetzugang erfassen. Man spricht hier von dem sogenannten Logfile oder Weblog. Das sind die gleichen Daten, die Sie bei jeder Internetseite zwingend hinterlassen, die Sie aufrufen. Im Mittelpunkt steht die IP-Adresse, von der aus Sie unsere Seiten aufrufen. An diese Internetadresse schickt der Webserver Ihnen die Daten, die Sie sehen wollen. Die Nutzungsprotokollierung erfasst diese Daten in Zusammenhang mit einem Zeitstempel.

Datenverarbeitungen durch die einzelnen Anwendungen innerhalb des digitalen Arbeitsplatzes: Die Module von openDesk erfassen und speichern Daten in dem für solche Anwendungen typischen Umfang:

- Das E-Mail-Modul speichert neben Metadaten zu Sender und Empfänger die Inhalte und Anhänge der gesendeten und empfangenen E-Mails;
- gleiches gilt für das Nachrichten-Modul;
- das Videokonferenz-Modul überträgt das Bild- und Tonsignal, das von Kamera und Mikrofone Ihres Endgeräts aufgenommen und der Anwendung (mit Ihrer Zustimmung) bereitgestellt wird, sowie Äußerungen im begleitenden Chat;
- der Dateispeicher speichert Dateien unterschiedlichster Art, in deren Inhalten personenbezogene Daten jeder Art enthalten sein können

5.2. Datenkategorien

Datenarten innerhalb der Nutzungsprotokollierung:

- IP-Adresse, von der aus openDesk aufgerufen wurde
- Datum und Uhrzeit des Zugriffs
- in openDesk, die im Browser aufgerufen werden
- Art und Version des Internetbrowsers
- Art und Version des Betriebssystems

Datenarten innerhalb der Anwendungsnutzung:

- Namen und Kontaktdaten (Adressen, Telefonnummern, E-Mail-Adressen)
- Kommunikations- und Rechercheinhalte (in E-Mails, Schreiben/ Akten, Notizen, Nachrichten, Videokonferenzen)
- Termine
- Bild-, Video- und Tonaufnahmen (als Dateien, die in openDesk gespeichert werden)

Abhängig vom Aufgabenbereich der openDesk-Nutzenden können die Kommunikations- und Rechercheinhalte personenbezogene Daten jeder Art umfassen, also auch besonders schützenswerte Daten nach Art. 9 DSGVO wie z.B. Gesundheitsdaten oder nach Art. 10 DSGVO zu Strafverfahren.

5.3. Datenempfänger (ggf. Drittstaatentransfer)

Zentrum für Digitale Souveränität der Öffentlichen Verwaltung GmbH (ZenDiS) als Anbieter des openDesk-SaaS-Dienstes und Unterauftragnehmer des ZenDiS. Die Dienstleister sind über einen Auftragsverarbeitungsvertrag auf den Datenschutz verpflichtet ist. Ein Drittstaatentransfer findet nicht statt.

Im Falle von Angriffen auf openDesk Weitergabe an von uns beauftragte Forensiker und Ermittlungsbehörden.

5.4. Zweck und Rechtsgrundlage

Der Zweck der Datenverarbeitung ist die Nutzung von openDesk als browserbasierte Onlineanwendung (Software-as-a-Service) im Sinne eines digitalen Arbeitsplatzes mit

verschiedenen Funktionsmodulen sowie Nachforschungen, sollte es zu einem unrechtmäßigen Zugriff auf openDesk kommen (z.B. einen Hackerangriff).

Rechtsgrundlage ist Erfüllung des Beschäftigungverhältnisses, in dessen Rahmen den Nutzenden ein Zugangskonto zur Verfügung gestellt wird. Die Nutzung des digitalen Arbeitsplatzes zählt zu den technischen Gegebenheiten des Beschäftigungsverhältnisses. Für den speziellen Falle eines Angriffs auf openDesk steht dem Verantwortlichen ein berechtigtes Interesse zu, den Ermittlern Indizien dafür bieten zu können, wie sich der Angriff abgespielt hat.

5.5. Speicherdauer

Hinweis: Hier ist vom Betreiber des Mandanten die gewählte Speicherdauer anzugeben.

6. Begleitende Dokumentation

Die Anwendung openDesk wird Anwendenden vorgestellt auf https://docs.opendesk.eu/.

7. Datensicherheit und Risikoadäquanz (Art. 24, 25, 32 DSGVO)

7.1. Einleitung Risiko und Adäquanz

Die DSGVO verlangt an verschiedenen Stellen, dass die Verarbeitung personenbezogener Daten in sicherer Weise erfolgen muss. Diese Pflicht ergibt sich insbesondere aus den Art. 24, 25 und 32 DSGVO. Bei der Beurteilung dessen, was an Sicherheit erforderlich ist, sind nach Maßgabe der DSGVO zu berücksichtigen die Art, der Umfang, die Umstände und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der Betroffenen (Art. 24 DSGVO). Ebenfalls zu berücksichtigen sind der Stand der Technik und die Implementierungskosten der Maßnahmen (Art. 25 Abs. 1 und Art. 32 DSGVO).

Art. 32 Abs. 2 DSGVO unterstreicht die Relevanz der Gewährleistungsziele, wie man sie auch aus der Informationssicherheit kennt: Schutz gegen Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise Zugang zu personenbezogenen Daten. Mit anderen Worten geht es um Vertraulichkeit, Richtigkeit und Verfügbarkeit (siehe auch die entsprechenden Datenschutzgrundsätze in Art. 5 Abs. 1 d und f DSGVO).

7.1.1. Fokus auf Betroffene

Datensicherheit nach DSGVO unterscheidet sich von der Informationssicherheit, wie sie z.B. im BSI-Gesetz geregelt ist, durch die Person, die geschützt wird. Die Informationssicherheit dient dem Schutz der Organisation, also z.B. der Institution, die Betreiberin des openDesk-Mandanten ist. Die Datensicherheit dient dem Schutz der Betroffenen, also der Personen, deren Daten von den Verantwortlichen verarbeitet werden.

In diesem Sinne sind sowohl die Risiken aus Sicht der Betroffenen und nicht des Verantwortlichen zu bestimmen und auch die Wahrscheinlichkeit und Schwere eines Schadenseintritts sind aus Sicht der Betroffenen zu beurteilen.

7.1.2. Datenschutzrisiken und Schutzbedarf nach Informationssicherheit

Für die Informationssicherheit gibt es das Konzept der drei Schutzbedarfskategorien normal, hoch und sehr hoch. Die DSGVO kennt diese Kategorien nicht. Das Datenschutzrecht beschreibt die Risiken als kein oder nur geringes Risiko, normales Risiko oder hohes Risiko. Im Standarddatenschutzmodell („SDM“), das von der DSK als Methode in Anlehnung an die IT-Grundschutz-Methodik des Bundesamts für die Sicherheit in der Informationstechnik („BSI“) entwickelt wurde, wurde hierzu eine Zuordnung festgehalten.

- Das geringe und das normale Risiko aus der Datenschutzperspektive entsprechen dem normalen Schutzbedarf aus der Informationssicherheit.
- Das hohe Risiko im Datenschutz entspricht dem hohen Schutzbedarf.
- Dementsprechend gibt es aus dem Datenschutzrecht keine Entsprechung zum sehr hohen Schutzbedarf in der Informationssicherheit.

Die Definitionen zur Einstufung der Schutzbedarfskategorien verweisen auch auf personenbezogene Aspekte. Für den Schutzbedarf sehr hoch betrifft das Gefahren für die körperliche Unversertheit (Gesundheit und Leben). In bestimmten Zusammenhängen kann sich an die Offenbarung eines personenbezogenen Datums eine extreme Gefahr für die körperliche Unversertheit anschließen, z.B. wenn der Aufenthalt einer von aggressivem Stalking betroffenen Person ihrem Verfolger offenbart wird. In solchen Konstellationen ist aus der Informationssicherheit z.B. für schutzgewährende Einrichtungen ein sehr hoher Schutzbedarf mit Blick auf die Daten zum Aufenthalt der Person anzunehmen. Da der Schutz aber nicht dem Rechtsgut der informationellen Selbstbestimmung dient, sondern dem Schutz der körperlichen Unversertheit aus Art. 2 Abs. 2 Grundgesetz, bedarf es aus DSGVO-Perspektive keines Pendants zum entsprechenden Schutzbedarf.

7.1.3. Ergänzende Gewährleistungsziele

Die Informationssicherheit kennt nur die drei Gewährleistungsziele Vertraulichkeit, Integrität (Richtigkeit) und Verfügbarkeit. Diese drei Ziele sind auch in der Datensicherheit von herausragender Bedeutung. Der Datenschutz kennt zusätzlich vier weitere Gewährleistungsziele: Datenminimierung, Nichtverkettung, Intervenierbarkeit und Transparenz

7.1.4. Definition Risiko

Ein Datenschutzrisiko ist jede Gefährdung für eins der sieben Gewährleistungsziele.

7.2. Datenschutzrisiken durch diese Verarbeitung

Risiken und Zuordnung auf die beteiligten Verantwortlichen und Auftragsverarbeiter

Gewährleistungsziel	Risiko aus Sicht der Betroffenen	Zuständigkeit
Vertraulichkeit	Offenbarung der Datenbankinhalte mit Bezug auf die betroffene Person (z.B. in E-Mails, Kontakte, Kalender, Dateien, Aufgaben, u.a.)	DSGVO-Verantwortliche (Berechtigungsmanagement, Verpflichtung + Schulung Nutzende), ZenDiS (Sicherheitsarchitektur), B1 Systems (Support), STACKIT (Hosting)
Vertraulichkeit	Offenbarung personenbezogener Nutzungsprotokolle gegenüber Unberechtigten	DSGVO-Verantwortliche, ZenDiS (Protokollierungskonzept), B1 Systems (Support), STACKIT (Hosting)
Richtigkeit	Ungewollte bzw. unberechtigte Veränderungen der Datenbankinhalte	Nutzende, ZenDiS, B1, STACKIT
Richtigkeit	Fehlerhafte Darstellung der Datenbankinhalte	ZenDiS (Anwendungsarchitektur), B1 Systems (Support), STACKIT (Hosting)
Richtigkeit	Fehlerhafte Nutzungsprotokollierung	ZenDiS (Protokollierungskonzept), B1 Systems (Support), STACKIT (Hosting)
Verfügbarkeit	Verlust der Datenbankinhalte	ZenDiS (Sicherheitsarchitektur), B1 Systems (Support), STACKIT (Hosting)
Verfügbarkeit	Zugriffsverweigerung auf Datenbankinhalte	ZenDiS (Sicherheitsarchitektur), B1 Systems (Support), STACKIT (Hosting)
Datenminimierung	Übermäßige Nutzungsprotokollierung	ZenDiS (Protokollierungskonzept)
Nichtverkettung	Verknüpfung der Nutzungsaktivität	ZenDiS (Protokollierungskonzept),

	mit anderen Daten	B1 Systems (Support), STACKIT (Hosting)
Intervenierbarkeit	Mangelhafter Umgang mit Betroffenenrechten	DSGVO-Verantwortliche
Transparenz	Mangelhafte Datenschutzinformation	DSGVO-Verantwortliche

7.3. Schutzmaßnahmen und Zuordnung zu den Risiken

Risiko	Schutzmaßnahme
Offenbarung der Datenbankinhalte	Siehe Sicherheitskonzept der DSGVO-Verantwortlichen und des ZenDiS (TOMs zum AV-Vertrag)
Offenbarung der Nutzungsprotokolle	Siehe Protokollierungskonzept
Ungewollte bzw. unberechtigte Veränderungen der Datenbankinhalte	• Qualitätssicherungsstandards in der Anwendungsentwicklung • Im Übrigen: siehe Sicherheitskonzept der DSGVO-Verantwortlichen und des ZenDiS (TOMs zum AV-Vertrag)
Fehlerhafte Darstellung der Datenbankinhalte	• Qualitätssicherungsstandards in der Anwendungsentwicklung • Im Übrigen: siehe Sicherheitskonzept des ZenDiS (TOMs zum AV-Vertrag)
Fehlerhafte Nutzungsprotokollierung	Qualitätssicherungsstandards in der Anwendungsentwicklung
Verlust der Datenbankinhalte	Siehe Datensicherungskonzept
Zugriffsverweigerung auf Datenbankinhalte	Siehe Sicherheitskonzept des ZenDiS (TOMs zum AV-Vertrag)
Übermäßige Nutzungsprotokollierung	Siehe Protokollierungskonzept
Verknüpfung der Nutzungsaktivität Testender mit Vertriebsaktivitäten des ZenDiS	Siehe Protokollierungskonzept (organisatorisches und technisches Berechtigungskonzept für die Nutzungsprotokollierung, das den Zugang zu den Logfiles auf einen kleinstmöglichen Kreis von Administrierenden beschränkt)
Mangelhafter Umgang mit Betroffenenrechten	Siehe Datenschutzkonzept der DSGVO-Verantwortlichen
Mangelhafte Datenschutzinformation	Siehe Datenschutzinformation der DSGVO-Verantwortlichen

7.4. Feststellung Risikoadäquanz

Die Risikoadäquanz ist abhängig von Maßgaben des Verantwortlichen zur Risikobeurteilung. Die Feststellung, ob die Nutzung des openDesk-Mandanten risikoadäquat ist, obliegt dem jeweiligen Betreiber eines openDesk-Mandanten.

8. Datenschutzfolgenabschätzung (Art. 35 DSGVO)

Eine Datenschutzfolgenabschätzung („DSFA“) nach Art. 35 DSGVO ist erforderlich, wenn eine Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Datenschutzrechte der Betroffenen zur Folge hat. Die Beurteilung, ob ein solches hohes Risiko vorliegt, erfolgt im Rahmen einer sogenannten Schwellwertanalyse.

Ist eine DSFA erforderlich, bedarf es der Zusammenstellung eines interdisziplinären DSFA-Teams, das in einem ersten Schritt alle potenziellen Risiken für die Datenschutzrechte der Betroffene durch die Verarbeitung zusammenstellt. Im zweiten Schritt sind die Risiken ohne Blick auf Schutzmaßnahmen nach Eintrittswahrscheinlichkeit und Schadensausmaß zu bewerten. Im dritten Schritt sind die ergriffenen Schutzmaßnahmen den einzelnen Risiken zuzuordnen und die Risiken anschließend erneut nach Eintrittswahrscheinlichkeit und Schadensausmaß – jetzt unter Berücksichtigung der Schutzwirkung der Maßnahmen – zu bewerten.

Führt die Bewertung unter Einbeziehung der Schutzmaßnahmen dazu, dass kein hohes Risiko mehr gegeben ist, kann die Verarbeitung stattfinden. Sollten die Risiken der geplanten Verarbeitung auch unter Einbeziehung der Schutzmaßnahmen weiterhin ein hohes Risiko darstellen, sind weitere risikominimierende Maßnahmen zu ergreifen, die Datenschutzaufsicht gemäß Art. 36 DSGVO zu konsultieren oder auf die geplante Verarbeitung zu verzichten.

Art. 35 Abs. 1 DSGVO nennt beispielhaft Kriterien, wann ein hohes Risiko vorliegen könnte. Art. 35 Abs. 3 DSGVO nennt drei konkrete Konstellationen, in denen eine DSFA erforderlich ist. Hiervon trifft keine auf eine Anwendung wie openDesk zu.

Der Europäische Datenschutzausschuss („EDSA“) hat bereits 2017 das Working Paper 248 veröffentlicht, das neun typische Kriterien nennt, die im Rahmen einer Schwellwertanalyse betrachtet werden sollten. Sollten zwei der neun Kriterien erfüllt sein, sei regelmäßig von der Erforderlichkeit einer DSFA auszugehen.

Ergänzend gibt es eine Liste der Bundesdatenschutzbeauftragten („BfDI“) und vergleichbare Listen weiterer Datenschutzaufsichtsbehörden nach Art. 35 Abs. 4 DSGVO, die für bestimmte Verarbeitungsvorgänge eine DSFA vorschreiben.

Ob die Nutzung des openDesk-Mandanten mindestens zwei Kriterien nach dem Katalog des EDSA erfüllt oder die Verarbeitung einem Vorgang auf der Liste der

Aufsichtsbehörden entspricht, muss jeder Verantwortliche mit Blick auf die eigene Nutzung des openDesk-Mandanten beurteilen. Sollte eine solche Prüfung zu dem Ergebnis kommen, dass eine DSFA für die Nutzung des openDesk-Mandanten erforderlich ist, ist diese durchzuführen und zu dokumentieren.

9. Fazit

Die Nutzung der openDesk-Lösung, wie ZenDiS sie zur Verfügung stellt, erfolgt datenschutzkonform.